Gordon Gibby MD KX4Z
Newberry, FL

July 20, 2019

RE: RM-11831
- Reply to Ron Kolarik https://ecfsapi.fcc.gov/file/1071758880862/Reply%20to%20Gibby%20comments.pdf
- Additional Comments, citing numerous requests for completed demonstration

Gentlemen:

I was pleasantly surprised to read the recent comments by the Petitioner, (https://ecfsapi.fcc.gov/file/1071758880862/Reply%20to%20Gibby%20comments.pdf) wherein he now indicates that the "broader intent of RM-11831 [is that] all modes **must be open to understanding** by *simply owning the proper equipment or digital decoding software.*" [emphasis added]

In this filing, I will attempt to address:
1. That Mr. Kolarik's eavesdropping demands are actually now proven quite possible without regulatory changes;
2. Mr. Kolarik's confusion on the qualifiers that apply to a simple proof-of-concept, versus the full software he requires;
3. Being spied-upon is not necessarily a proof of wrongdoing; and
4. Prior claims that the demonstration would end this crusade.

1. Eavesdropping Requires No Regulatory Changes

Despite the many other statements in the cited filing, it has already now been shown that Mr. Kolarik's requirement are very likely achievable in an engineering effort, and have been for quite some time, for current modulations, without a single change to the existing regulations. I'm not certain that Mr. Kolarik is seeing what has been shown, in filings here[1] [2] [3] [4] [5]and in available

1 How to monitor any ARQ pactor communication, https://ecfsapi.fcc.gov/file/10512224804129/SCS_FCC_Reply_RM11831.pdf
2 Description of first complete text eavesdropping of a WINLINK message to prove there is no encryption, https://ecfsapi.fcc.gov/file/10410170249078/FCCRM11831-4.pdf
3 Offer of free PACTOR monitoring tool https://ecfsapi.fcc.gov/file/10417301289214/SCS_FCC_Comment_RM11831.pdf
4 Documentation of additional, including witnessed, full text eavesdroppings of WINLINK messages: https://ecfsapi.fcc.gov/file/1071540521688/FCCCommentJuly2019.pdf
5 Witness account of successful full text WINLINK eavesdropping: https://www.fcc.gov/ecfs/filing/10715183432187

texts.[6] [7]

Quite a bit of ink was spilled in Chapter 1 of the published text Spying On WINLINK explaining precisely how a radio amateur could understand all WINLINK transmissions **if they owned the proper equipment and digital decoding software**. No change in any regulation is required for Mr. Kolarik's request to have this eavesdropping capability– but those who wish those capabilities may have to *develop* some equipment and some software! Some of them are recognized experts in matters of radio communications, so that should not be difficult for them.

As Chapter 1 of Spying On WINLINK explained, a likely method allow Mr. Kolarik to do what he wants, is to obtain the following items in his approved categories:

Proper Equipment

- Procure ownership or access to multiple receivers, antennas, etc., in geographically diverse locations
- Have those receiving systems equipped with the necessary tools to receive the desired signals (e.g., PACTOR modem, sound-card system, protocol software, etc.), that handle ISO layers 2-3. [8]

Proper digital decoding software

- Utilize application software at ISO levels 4 and above that links those receiving systems to a display, so that good packets of whatever protocol is being monitored (WINMOR, PACTOR, ARDOP, AX.25, and so forth) are identified, placed in proper order, and then decompressed using (publicly available) decompression software.[9]

Based on the work that has already been demonstrated, and on statements form world-renowned experts, this is now quite possible, and those who desire it so strongly should immediately begin to bring it about.

However, I'm not optimistic that many will put actual work into their goal, **given that the same messages (for WINLINK) are available on a web viewer[10] for licensed amateurs (or anyone else whom the WINLINK group (or presumably the FCC) wishes to provide access).** I would assume that the FCC could demand access permanently for any group of viewers they chose.

So the path is already clear (and indeed, has been for some years) for Mr. Kolarik to have his request, for WINLINK transmissions, and another large target has not appeared. Therefore, no

6 Commercially available text documenting methods to eavesdrop on WINLINK and of the successful proof-of-concept https://www.amazon.com/Spying-WINLINK-Gordon-L-Gibby/dp/1080563199

7 Freely available PDF (for non-commercial usage) of Spying On WINLINK: https://www.qsl.net/nf4rc/2019/SpyingOnWINLINKV2.pdf

8 For example, PACTOR modems are commercially available; the WINMOR software TNC is available https://downloads.winlink.org/User%20Programs/Winmor_TNC_install_1-5-13-0.zip the ARDOP software TNC is available http://www.cantab.net/users/john.wiseman/Downloads/Beta/ and the VARA software TNC is available at https://rosmodem.wordpress.com/

9 John Huggins (https://www.fcc.gov/ecfs/filing/10719145238785) has already embarked on that task and has demonstrated capture of PACTOR packets, precisely as predicted by SCS experts.

10 USA Amateur WINLINK viewer: https://winlink.org/content/us_amateur_radio_message_viewer

regulatory changes are indicated.

2. Petitioner's Confusion

Mr. Kolarik begins his filing with a concern that the eavesdropper should not have to go through all the efforts detailed in my filings...obviously confusing a proof-of-concept experiment done without a stitch of software development, with a finished application that could have been built in the past years to meet his demands.

This confusion continues. In the remainder of that filing, he confuses which engineering constraints apply to the completed proof-of-concept, versus those which would need to be observed by those building a full-scale eavesdropping system, as he demands.

The following table attempts to disentangle the various qualifiers that the Petitioner cites, all mixed together, into their proper categories:[11]

Kolarik's listed qualifiers that apply to the radio-wave monitoring system Mr. Kolarik desires.	**Kolarik's listed qualifiers that apply to the proof-of-concept experiments**.
#1 If all packets are not copied with 100% accuracy, no decode is possible.-- Applies	#1 If all packets are not copied with 100% accuracy, no decode is possible – Applies
#2 as listed by Kolarik DOES NOT APPLY	#2 If the calls of the stations involved are not known in advance no decode is possible. -- Close. Actually, only the intended recipient call need be known
#3 as listed by Kolarik DOES NOT APPLY	#3 If the monitoring station is not closely in sync (milliseconds) with the sending stations no decode is possible. This part "is largely luck!!!!" Applies.
#3 [sic] [12] If a widely dispersed network of receiving stations are able to copy the packets – Likely: this may be the optimal solution, however sometimes only one station will be needed.	#3 [sic] as listed by Kolarik DID NOT APPLY to the proof-of-concept experiment.
#4 If custom software is written to combine all the received "diversity packets" – Applies	#4 as listed by Kolarik DID NOT APPLY to the proof-of-concept experiment [which used off the shelf free software]

#5 as listed by Mr. Kolarik ("IF any compression is applied, and the method known, decoding may be possible") is now superfluous, because copying the packets (#1 above) and then simply

11 Mr. Kolarik's filing contains two #3 qualifiers.

12 Mr. Kolarik has two #3's in his listing of qualifiers.

routing them in proper order to the known public decompression algorithm suffices.

After such loud claims that Forward Error Correction would solve all accuracy problems[13], with no need for ARQ, it is now surprising that there is not wide acknowledgment that the FEC already utilized by PACTOR modems actually makes the task of reassembling 100% correct packets that much easier. Nevertheless, a widescale snooping monitor will likely benefit from having diversity reception; at some point additional receivers will overcome the handicap of not having independent ability to request repeats. With modern web-based SDR receivers and so many urgently-concerned volunteers, this should have been done quite a while ago.

3. Eavesdropping, Spying, Snooping and Implications

Mr. Kolarik then is concerned by the use of the words "spying" and "snooping."

> *The title of the original article "Spying on Winlink" and the constant use of the words, spying and snooping, throughout the document implies the transmissions are secret (spying) or private (snooping).*

Yet in his original Petition, he chose the largely synonymous word "eavesdropping" and then demanded that it be possible! Now he is alleging that an eavesdropper spying on others conducting ordinary emails proves *the emailers* are doing something in secret? Odd.

Obviously all WINLINK communications are now conclusively proven, both by simple examination of the public linbpq code[14] and by a simple practical experiment, to be transmitted as un-encrypted "clear text" which is compressed with an ancient and public domain algorithm. Further they are now available on a web page to peruse – the spying / snooping is not by the lawful participants in the communications, but is instead by persons wishing (also lawfully) to monitor those communications. This is amateur radio. Mr. Kolarik is free to listen in any anyone's amateur radio communications, but as he himself points out – you have to have the proper hardware and software in order to do it. As digital protocols become ever more efficient in the use of time, space and power, it may require ever more complicated hardware and software. Attempts to stifle progress are not ultimately desirable.

I'm not a party to the various other allegations of nefarious behavior on the part of others, that complete Mr. Kolarik's filing so I'll not address those.

4. Proof of the Concept Concluded: WINLINK can be monitored over the air

It is quite surprising that Mr. Kolarik and others are still making any argument at all, since so

13 See pp. 6-7 of https://ecfsapi.fcc.gov/file/10429199250117/FCC%20Letter%20Reply%20to%20Comments%20RM%2011831.pdf

14 Publicly available in multiple locations, including: http://www.cantab.net/users/john.wiseman/Downloads/LatestLinBPQSource.zip

many amateurs (including at least one prominent multiple Filer on RM-11831) demanded on a national amateur radio forum just such a proof of observability as has been completed. Several stated proof of over the air monitoring would end the argument, as follows.

NN3W on April 9 2019

> "Been following this and this is the crux of the issue. If the WL and PACTOR proponents would demonstrate that with commonly available software / hardware and with a minimal financial commitment (i.e., less than, say, $500), this form of communication can be monitored by outside, neutral individuals, it would be game, set, and match.
>
> The entirety of the battle from Ted's side is that the data cannot be decyphered by an average ham using average equipment.
>
> So, the best way to prove him wrong is to prove him wrong. " [15]

AB2RA (Janis Carlson) [16] [17] [18]

> "1. Either it will work or not in the demo. **If it works, its over.** Wouldn't "over" be nice for everybody?" [19] [emphasis added]

KA4DPO added

> "Either you can, or can not decode the contents of other peoples message transmissions over PACTOR III who are not in your network." [20]

N5RFX jumped on the bandwagon:

> "Do the demo! Do the demo! Do the demo! Mark N5RFX " [21]

N5RFX went further to say that he did not think anyone could do such a demonstration:

> "Oh I am serious. I want to see a demonstration. In my opinion, I don't think you or anyone else can do the demonstration. This not ad hominem, it is my opinion. I am also serious that in my opinion unattended operation on HF was a mistake, but I am no Don Quixote.
> Mark N5RFX" [22]

---

15 https://forums.qrz.com/index.php?threads/new-digital-petition-at-the-fcc-rm-11831.652589/page-67#post-5025767

16 https://ecfsapi.fcc.gov/file/1071863434533/FINAL%20VERSION%20Siddall%20reply%20June%2018.pdf

17 https://ecfsapi.fcc.gov/file/10510209788784/%24RM-11831%20may%2010%20reply.pdf

18 https://ecfsapi.fcc.gov/file/10330103611071/RM-11831%20FINAL%201.pdf

19 https://forums.qrz.com/index.php?threads/new-digital-petition-at-the-fcc-rm-11831.652589/page-68#post-5025920

20 https://forums.qrz.com/index.php?threads/new-digital-petition-at-the-fcc-rm-11831.652589/page-70#post-5026027

21 https://forums.qrz.com/index.php?threads/new-digital-petition-at-the-fcc-rm-11831.652589/page-70#post-5026046

22 https://forums.qrz.com/index.php?threads/new-digital-petition-at-the-fcc-rm-11831.652589/page-73#post-5026207

Janis Carlson weighed in again on April 9th 2019;

> "Helfert filed a letter with the FCC in 16-239.
> Said it was not an issue.
> Others have said Over The Air display of contents was possible, with a pile of technobabble bafflegab.
> Is it true or not, and a lot of people have figured that out, without a degree in computer science.
> Test it and prove it now, or admit that it isn't possible, and we can move to the next point.
> Over would be good." [23]

N1FM:

> "Unfortunately, no one has demonstrated that the messages sent over the air, via ham radio, are fully transparent.
>
> And plenty of folks have said they are not. Hence the petition." [24]

N1FM cited the key question:

> "Yes, that's the million dollar question. You posted a slew of violations, that lead to other questions, but can we decrypt, er, decode the messages as well as the headers, or does using an SCS modem provide a level of obscurity and security to the data? " [25]

Now with a public record of decoding WINLINK PACTOR emails five times, will all these persons acknowledge that this is merely an engineering project?

Sincerely,

Gordon L. Gibby MD KX4Z

23 https://forums.qrz.com/index.php?threads/new-digital-petition-at-the-fcc-rm-11831.652589/page-75#post-5026290

24 https://forums.qrz.com/index.php?threads/new-digital-petition-at-the-fcc-rm-11831.652589/page-80#post-5026729

25 https://forums.qrz.com/index.php?threads/new-digital-petition-at-the-fcc-rm-11831.652589/page-88#post-5027203